UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/826,814	04/16/2004	G. Glenn Henry	CNTR.2226	1576

23669 7590 04/23/2008
HUFFMAN LAW GROUP, P.C.
1900 MESA AVE.
COLORADO SPRINGS, CO 80906

EXAMINER	
HOANG, DANIEL L	
ART UNIT	PAPER NUMBER
2136	
NOTIFICATION DATE	DELIVERY MODE
04/23/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO@HUFFMANLAW.NET

Office Action Summary	**Application No.** 10/826,814	**Applicant(s)** HENRY ET AL.	
	Examiner DANIEL L. HOANG	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

CLAIMS PRESENTED

Claims 1-34 are presented.

RESPONSE TO AMENDMENTS

In response to applicant's amendments regarding the previous action's 112 rejections, said rejections have been appropriately withdrawn.

RESPONSE TO ARGUMENTS

Applicant's arguments with respect to claims 1, 22, and 28 have been considered but are moot in view of the new ground(s) of rejection.

CLAIM REJECTIONS

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-5, 10-11, 13-22, 25-28, 31-34, are rejected under 35 U.S.C. 103(a) as being unpatentable over Yup et al., US PGP No. 20020191784, and further in view of Best, US Patent No. 4,168,396.

As per claim 1, 22, 28, Yup teaches:

An apparatus for performing cryptographic operations, comprising:

a cryptographic instruction, received by a computing device microprocessor as part of an instruction flow executing on said computing device microprocessor, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said one of the cryptographic operations comprises:

[see paragraphs 0038-0039]

a plurality of CBC block cryptographic operations performed on a corresponding plurality of input text blocks;

[see paragraph 0040]

[CBC] mode logic, operatively coupled to said cryptographic instruction, configured to direct said computing device microprocessor to update pointer registers and intermediate results for each of said plurality of [CBC] block cryptographic operations; and

[see paragraph 0025]

execution logic, operatively coupled to said [CBC] block pointer logic, configured to execute said one of the cryptographic operations.

[see paragraph 0041]

Yup is not explicit in teaching CBC block cryptographic operations. More specifically, although Yup teaches cryptographic operations on multiple successive blocks of text, Yup does not expressly state that these cryptographic operations are of cipher block chaining mode. As evident in applicant's disclosure on paragraph 0012 of the specification, it is well known that all symmetric key algorithms employ the same types of modes. ECB, CBC, CFB, and OFB are examples that applicant discloses. Based on this, examiner deems it obvious for one of ordinary skill in the art to implement CBC or any other block cipher mode in conjunction with the system/apparatus taught by Yup.

Yup is also not explicit in teaching that the computing device is a microprocessor. For this limitation, examiner relies on the Best reference. Please see col. 2, lines 67-68 and col. 3, lines 1-12. Best teaches a microprocessor for executing computer programs which have been enciphered during manufacture to deter the execution of the programs in unauthorized computers. This microprocessor deciphers and executes an enciphered program one instruction at a time, through a combination of substitutions, transpositions, and exclusive-OR additions, in which the address of each instruction is combined with the instruction. It would have been obvious at the time of the invention to one of ordinary skill in the art to implement the invention cited above by Yup within a microprocessor, as taught by Best, in order to provide a secure cryptographic system which is suitable for protecting programs which are deciphered one byte at a time as the program executes.

As per claim 2, Yup teaches:

The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises: a CBC mode encryption operation, said CBC mode encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks.

[see paragraph 0040]

As per claim 3, 32, Yup teaches:

The apparatus as recited in claim 1, wherein said one of the cryptographic operations further comprises: a CBC mode decryption operation, said CBC mode decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks.

[see paragraph 0040]

As per claim 4, 33, Yup teaches:

The apparatus as recited in claim 1, wherein said one of the cryptographic operations is accomplished according to the Advanced Encryption Standard (AES) algorithm.

[see paragraph 0024]

As per claim 5, 34, Yup teaches:

The apparatus as recited in claim 1, wherein said cryptographic instruction prescribes that cipher block chaining mode to be employed in accomplishing said one of the cryptographic operations.

[see rejection of claim 1]

As per claim 10, 25, Yup teaches:

The apparatus as recited in claim 1, wherein said CBC mode logic directs said computing device to modify said pointer registers to point to next input and output text blocks at the completion of each of said plurality of CBC block cryptographic operations on each of said corresponding plurality of input text blocks.

[see paragraphs 0025-0027]

As per claim 11, 26, Yup teaches:

The apparatus as recited in claim 1, wherein said CBC mode logic directs said computing device to store a current output text block to a memory location pointed to by an initialization vector register.

[see paragraphs 0043-0044]

As per claim 13, 27, 31:

Yup does not explicitly disclose:

> The apparatus as recited in claim 1, wherein said cryptographic instruction is prescribed according to the x86 instruction format.

It would have been obvious to one or ordinary skill in the art to create the instructions in x86 format or any other format. One would have been motivated to do so in order to conform to the type of platform selected for implementation of the encryption/decryption device.

As per claim 14, Yup teaches:

The apparatus as recited in claim 1, wherein said cryptographic instruction implicitly references a plurality of registers within said computing device.

[see paragraph 0024]

As per claim 15, Yup teaches:

The apparatus as recited in claim 14, wherein said plurality of registers comprises: a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of said plurality of input text blocks upon which said one of the cryptographic operations is to be accomplished.

[see paragraphs 0024-0027]

As per claim 16, Yup teaches:

The apparatus as recited in claim 14, wherein said plurality of registers comprises: a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks.

[see paragraphs 0024-0027]

As per claim 17, Yup teaches:

The apparatus as recited in claim 14, wherein said plurality of registers comprises: a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks.

[see paragraphs 0024-0027]

As per claim 18, Yup teaches:

The apparatus as recited in claim 14, wherein said plurality of registers comprises: a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations.

[see paragraphs 0024-0027]

As per claim 19, Yup teaches:

The apparatus as recited in claim 14, wherein said plurality of registers comprises: a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory for access of an initialization vector for use in accomplishing said one of the cryptographic operations.

[see paragraphs 0024-0027]

As per claim 20, Yup teaches:

The apparatus as recited in claim 14, wherein said plurality of registers comprises: a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations.

[see paragraphs 0024-0027]

Claims 6-9, 12, 23-24, 29-30, are rejected under 35 U.S.C. 103(a) as being unpatentable over Yup and Best as applied to claim 1 above, and further in view of Sorimachi et al., US Patent No. 7184549.

As per claim 6, 23, 29:

The Yup reference has been discussed above. Yup is not explicit in teaching:

> The apparatus as recited in claim 1, further comprising: a bit, coupled to said execution logic, configured to indicate whether said one of the cryptographic operations has been interrupted by an interrupting event.

Sorimachi teaches the deficiencies of Yup. *[see col. 13, lines 29-55]*

It would have been obvious to one of ordinary skill in the art to combine what is taught above by Sorimachi with the teachings of Yup in order to handle the exceptions when they occur. It would be beneficial to incorporate the use of exception handling so that the system can deal with exceptions in the event that a change in the normal flow of execution of the system arises.

As per claim 7, Sorimachi teaches:

The apparatus as recited in claim 6, wherein said bit is contained within a flags register.

[see col. 14, lines 28-45]

As per claim 8, Sorimachi teaches:

The apparatus as recited in claim 6, wherein said interrupting event comprises a transfer of program control to a program flow configured to process said interrupting event, and wherein execution of said one of the cryptographic operations on a current input text block is interrupted.

[see col. 14, lines 28-45]

As per claim 9, 24, 30, Sorimachi teaches:

The apparatus as recited in claim 8, wherein, upon return of program control to said cryptographic instruction, said one of the cryptographic operations is performed on said current input text block.

[see col. 14, lines 28-45]

As per claim 12, Sorimachi teaches:

The apparatus as recited in claim 6, wherein said interrupting event comprises an interrupt, an exception, a page fault, or a task switch.

[see col. 13, lines 29-55]

CONCLUSION

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

POINTS OF CONTACT

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Daniel L. Hoang/

Examiner, Art Unit 2136

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136